PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-146631
(43)Date of publication of application : 18.06.1988

(51)Int.Cl. H04L 9/04
G09C 1/00

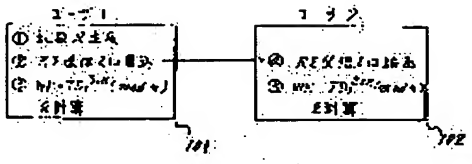
(21)Application number : 61-295342
(22)Date of filing : 10.12.1986

(71)Applicant : NEC CORP
(72)Inventor : OKAMOTO EIJI

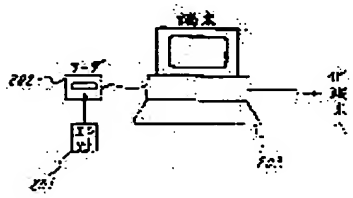
(54) KEY GENERATING DEVICE

(57)Abstract:

PURPOSE: To generate a cryptographic key with high in sccrecy by converting a random number selected at random, a select code preserved by it own equipment only, identification information of opposite station and a common code to all stations by predetermined conversion.



CONSTITUTION: Identification information IDi of a user (1) is the result of coding public information such as name, address and telephone number to identify the user (1). Moreover, a secret integer Si processed by the user (1) only and product (n) of plural primes are calculated by a credible manager and arranged in advance to the user (1). The user (1) inputs a cryptographic communication request to a terminal equipment 203 and loads an IC card 201 to a reader 202. The terminal equipment generates a random number R, reads the S1 and (n) from the IC card 201 to generate a work key wk, which ciphers a message desired to be sent and the result is sent to the user 2 together with the number R.



In receiving the R and the ciphered message, the user 2 reads the S1 and (n) from the IC card to generate the work key wk. Then the wk is used to decode the sent ciphered message into the original plain sentence.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－146631

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)6月18日
H 04 L 9/04		7240－5K	
G 09 C 1/00		7368－5B	

審査請求　未請求　発明の数 2　（全4頁）

㊹発明の名称　キー生成装置

㉑特　願　昭61－295342

㉒出　願　昭61(1986)12月10日

㉒発明者　岡本　栄司　東京都港区芝5丁目33番1号　日本電気株式会社内

㉑出願人　日本電気株式会社　東京都港区芝5丁目33番1号

㉔代理人　弁理士　内原　晋

明　細　書

発明の名称

キー生成装置

特許請求の範囲

1.複数の局から成る通信ネットワークの1つの局と他の局との間の暗号用のキーを生成するキー生成装置において、ランダムに選ばれた乱数と、自局のみが保有する秘密コードと、相手局の識別情報と、全局に共通なコードとをあらかじめ定められた変換で変換して前記暗号用のキーを生成することを特徴とするキー生成装置。

2.記録情報を暗号化あるいは復号化するときのキーを生成するキー生成装置において、ランダムに選ばれた乱数と、ユーザ固有の秘密コードと、全ユーザに共通なコードと、ユーザ識別情報とをあらかじめ定められた変換で変換して前記キーを生成することを特徴とするキー生成装置。

発明の詳細な説明

〔産業上の利用分野〕

本発明は通信暗号あるいはファイル暗号に用いるキーを生成するキー生成装置に関する。

〔従来の技術〕

キー生成装置として従来から知られているものの1つに、公開鍵配送方式を用いたキー生成装置がある。この方式はアイ・イー・イー・イー・トランザクションズ・オン・インフォーメーション・セオリー（IEEE Transactions on Information Theory)22巻 6号 644頁～ 654頁に掲載されている。

このキー生成装置は各通信者（またはファイルの書込者や読出者，以下通信者に含める）に対応した公開情報を必要とし、例えば通信者Aが通信者Bと暗号通信する場合には、AはBの公開情報Y_BとAのみの秘密情報X_Aから$Y_B^{X_A}$（mod p）により暗号キーwkを作成する。ここで、pは公開されている大きな素数（256ビット程

度）であり、a（mod　b）はaをbで割った余りを示す。Bは同様にY_A^{X_B}（mod　p）によりwkを作成する。

ここでY_B^{X_A}（mod　p）＝Y_A^{X_B}（mod　p）となるようにY_A＝α^{X_A}（mod　p），Y_B＝α^{X_B}（mod　p）と定められている。αは定数。

Y_Aとαとpがわかっていても、Y_A＝α^{X_A}（mod　p）をみたすX_Aを求めることは困難であること、即ち、いわゆるディスクリート・ログリズムの困難さが前記文献に記載されている。

〔発明が解決しようとする問題点〕

前記の従来のキー生成装置では、各通信者に対応する公開情報が必要となり、メンバーが増加すれば公開情報のリストも増加する。また、改ざんなども防止するための管理が必要となる。これらの欠点はファイル暗号の時も同様に存在する。

本発明の目的は、簡単な手段により上記欠点を除去し、機密性の高い暗号用のキーを生成することのできるキー生成装置を提供することにある。

〔問題点を解決するための手段〕

第１の発明のキー生成装置の構成は、複数の局から成る通信ネットワークの１つの局と他の局との間の暗号用のキーを生成するキー生成装置において、ランダムに選ばれた乱数と、自局のみが保有する秘密コードと、相手局の識別情報と、全局に共通なコードとをあらかじめ定められた変換で変換して前記暗号用のキーを生成することを特徴とする。

第２の発明のキー生成装置の構成は、記録情報を暗号化あるいは復号化するときのキーを生成するキー生成装置において、ランダムに選ばれた乱数と、ユーザ固有の秘密コードと、全ユーザに共通なコードと、ユーザ識別情報とをあらかじめ定められた変換で変換してキーを生成することを特徴とする。

〔実施例〕

第１図は第１および第２の発明の一実施例の原理を示すための図である。

第１の発明における局は端末，ユーザ等の通信主体であるが、第２の発明の主体であるユーザという言葉を共通に用いる。

第１図は第１の発明と第２の発明の共通原理を示している。キー配送の起動をかける側あるいはファイル書込を行なう側をユーザ１とし他方をユーザ２とする。ユーザ１は乱数Ｒを生成し、Ｒをユーザ２に送るか、ファイルの１部に書込む。

次に、暗号用のキー（以下ワークキーと言う）を、wk＝ID_2^{S_1R}（mod　n）で計算する。

ここで、nは複数の素数の積p_1 p_2 … p_kであり、約２００桁程度の大きな整数である。

また、ID_1はユーザ１の識別情報で、例えば、氏名，住所，電話番号など、ユーザｉを識別できる公開の情報をコード化して整数とみなしたものである。

さらに、S_1はユーザiのみが保有する秘密の整数である。これらのS_1，nは信頼できる管理者が計算してユーザｉにあらかじめ配っておく。この計算の仕方は後に示す。ユーザ２も同様にして、ワークキーwkを、wk＝ID_1^{S_2R}（mod　n）により計算する。ここで、ID_1とS_1の関係は

$$ID_1 = \alpha^{S_1} \pmod{n} \qquad (1)$$

となっている。αはある整数。このときユーザ１とユーザ２が計算したワークキーwkは、共にα^{S_1S_1R}（mod　n）に等しくなる。

ここで、ID_1，α，nがわかっても、nが大きいためにS_1を求めることができない。従って、ユーザ１とユーザ２以外の第３者がＲを知っても、α^{S_1S_2R}（mod　n）を作れない。これらは、ディスクリート・ログリズムの困難さによる。

一方、管理者はnの因数p_1，p_2，…p_kを各々小さくしておけば、任意のＩＤに対して

$$ID=\alpha^{x}\ (mod\ p) \qquad (2)$$

をみたすx」を計算できる。

ここで、αはmod　p」において生成元となるような任意の整数とする。

具体的なx」の計算法については、例えば第２０回アニュアル・シンポジウム・オン・ファウンデーションズ・オブ・コンピュータ・サイエンス（Annual Symposium on Foundations of Computer Science）予稿集の56頁～60頁（1979）に記載されている。

第２図は本発明の第１の実施例の構成を示すための図である。

ネットワークの端末２０３にＩＣカード・リーダ２０２が設置されている。ＩＣカード２０１は管理者が秘密のコードＳ，および公開の整数ｎを書き込んで各ユーザに配布したものである。

端末２０３がなすべき作業を第３図にフローチャートにして示す。ユーザ１がユーザ２に暗号通信を行なうものとして説明する。

ユーザ１は端末２０３に暗号通信要求を入力すると共に、ＩＣカード２０１をリーダ２０２に差込む。すると端末はユーザ１の正当性をチェックする。これは、ＩＣカードの正当性チェックを利用すればよく、例えば、暗証番号をＩＣカードの読み書きできないメモリエリアにＩＣカード製作段階に記入しておき、ユーザ１が端末に入力した暗証番号と一致するか否かでユーザ１の正当性を判定する。一致すれば、端末は乱数Ｒを生成し、ＩＣカード２０１からＳ，とｎを読込む。

ワークキーｗｋを式(1)に基づいて生成し、ワークキーｗｋで送りたいメッセージを暗号化して、その暗号文を前記Ｒと共にユーザ２へ送る。ユーザ２はＲと暗号文を受取ると、端末が同様にユーザ２の正当性をチェックし、チェックが肯定的になされた時は、ＩＣカードからＳ，とｎを読込んでワークキーｗｋを生成する。そして、そのｗｋを用いて送られた暗号文を元の平文に戻す。

第４図は第２の実施例の構成を示すための図である。第２図における端末２０３をフロッピーディスク付パーソナルコンピュータ（パソコン）としている。動作は第２図における通信文がフロッピーディスクへの記録文になったことだけである。但し、暗号化するユーザと復号化するユーザが同一であり得る点が、第２図と異なる。

本実施例において、フロッピーディスクやパソコンは一例にすぎず、他の記録媒体やコンピュータでもよい。

〔発明の効果〕

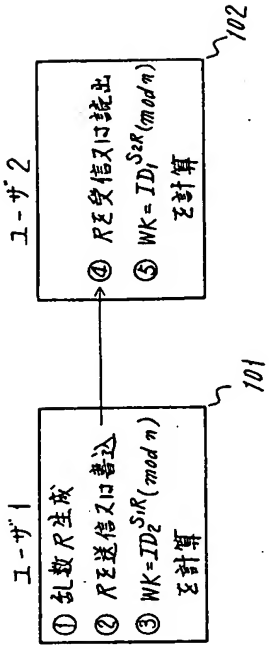
以上詳細に説明したように、本発明を用いれば、各ユーザに対応して公開情報をリストにしたテーブルが不要となる効果をもたらす。

図面の簡単な説明

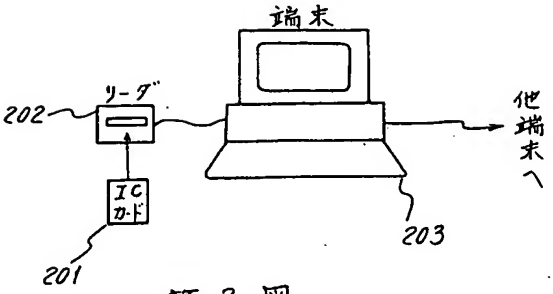
第１図は第１および第２の発明の実施例の原理を示すための図、第２図は第１の実施例の構成図、第３図は端末あるいはパソコンがなすべき作業のフローチャート、第４図は第２の実施例の構成図である。

１０１，１０２…ユーザ１，２がキー生成のために行なう処理、２０１，４０１…ＩＣカード、２０２，４０２…リーダ、２０３…端末、４０３…パソコン。

代理人　弁理士　内　原

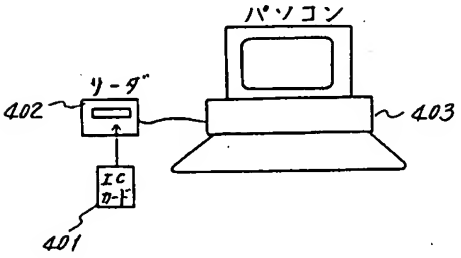


第1図



第2図

第4図



第3図